Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Discrete Applied Mathematics 128 (2003) 145–156
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Goppa-like bounds for the generalized Feng–Rao distances

J.I. Farrán[a,*], C. Munuera[b]

[a] *Departamento de Matemática Aplicada, ETSII, Universidad de Valladolid, 47011 Valladolid, Castilla, Spain*

[b] *Departamento de Matemática Aplicada, ETSA, Universidad de Valladolid, 47014 Valladolid, Castilla, Spain*

Received 8 February 2001; received in revised form 3 September 2001; accepted 8 April 2002

Abstract

We give some general bounds and formulas for the generalized Feng–Rao distances (or generalized order bounds) in an arbitrary numerical semigroup. The obtained results can be regarded as generalizations of well-known facts on the classical Feng–Rao distance (or first order bound), namely its connection with the Goppa distance. These results show that their asymptotical behaviour is essentially the same as in the case of the classical order bound. Explicit computations are given for the second Feng–Rao distance.
© 2003 Elsevier Science B.V. All rights reserved.

Keywords: Algebraic geometry codes; Weight hierarchy; Weierstrass semigroups; Goppa distance; Generalized Feng–Rao distance; Apéry sets

1. Introduction

Feng and Rao introduced in [5] a very efficient method for decoding the so-called *one-point algebraic geometry codes*. Such codes are defined as the duals of the evaluation codes given by linear maps of the type

$$ev_D : \mathscr{L}(mP) \to \mathbb{F}_q^n, \quad ev_D(f) = (f(P_1), \ldots, f(P_n)).$$

Here $P, P_1, \ldots, P_n$ are $n+1$ different rational points of a certain algebraic curve $\mathscr{X}$ defined over the finite field $\mathbb{F}_q$, $D = P_1 + \cdots + P_n$, and m is a positive integer (see [17]

* Corresponding author.
E-mail addresses: ignfar@wmatem.eis.uva.es (J.I. Farrán), cmunuera@modulor.arq.uva.es (C. Munuera).

0166-218X/03/$ - see front matter © 2003 Elsevier Science B.V. All rights reserved.
PII: S0166-218X(02)00441-9

for more details). The method of Feng and Rao decodes up to half the so-called *Feng–Rao distance*, and hence this number is a lower bound for the minimum distance of the corresponding code. This bound actually improves the Goppa estimate $d^* \doteq m+2-2g$, obtained from the Riemann–Roch theorem. More precisely, for the code $C=C_\Omega(D,mP)$ we have

$$d \equiv d(C) \geqslant \delta_{\mathrm{FR}}(m+1) \geqslant m+2-2g \quad \text{for } m > 2g-2.$$

The Feng–Rao distance is defined in terms of the Weierstrass semigroup of the curve $\mathscr{X}$ at P. Then, we can consider the problem of computing the Feng–Rao distance for arbitrary numerical semigroups. This problem has been successfully treated in the literature for different kinds of semigroups (see [3,4] or [13]).

On the other hand, the concept of minimum distance had been generalized to the *generalized Hamming weights*, which were independently introduced by Helleseth et al. [9] for the study of the weight distribution of codes over extensions of $\mathbb{F}_q$, and by Wei [18] motivated by applications from cryptography (the generalized Hamming weights completely characterize the performance of a linear code when used on the wire-tap channel of type II). Later, these weights have been shown to be useful also in trellis coding (lower bounding the number of trellis states), see [12], and in truncating and extending a linear code, see [10,16]. Also, they have been shown to be equivalent to another apparently different concept, the Forney's dimension/length profiles, see [6]. Thus, the close and deep connections of the Hamming weights with many topics studied in coding theory make them very interesting and attractive.

The natural generalization of the Feng–Rao bound to higher weights, which was called the *order bound*, was introduced in [8]. Unfortunately, the computation of these bounds turns out to be a very hard problem, and thus very few things are known about this subject. In this paper, we introduce some general results which generalize some well-known facts for the classical case of Feng and Rao. For example, regarding the Feng–Rao distance, it is a well-known fact that for $m \geqslant 2c-1$ we have

$$\delta_{\mathrm{FR}}(m) = m+1-2g$$

c being the conductor of the semigroup S. Denoting by $\delta^r_{\mathrm{FR}}(m)$ the rth order bound of $m \in S$, we show that also for $m \geqslant 2c-1$, we have

$$\delta^r_{\mathrm{FR}}(m) = m+1-2g+E_r$$

for a certain constant E_r depending on S and r. We prove that such a generalization of the Goppa estimate is a lower bound for the generalized Fen–Rao distance, provided that $m \geqslant c$. We give a result for symmetric semigroups which states that the above equality holds for half of the elements of the interval $[2g, 4g-2]$, generalizing a result given in [3] for the classical case. Finally, in Section 4 we give an effective method for computing the constant E_r when $r=2$.

2. Generalized Feng–Rao distances

Let S be a numerical semigroup, that is, a subsemigroup of $\mathbb{N}$ such that $\#(\mathbb{N}\setminus S) < \infty$ and $0 \in S$. Let $g \doteq \#(\mathbb{N} \setminus S)$ be the *genus* of S, and let $c \in S$ be its *conductor*, i.e.

the (unique) element $c \in S$ such that $c-1 \notin S$ and $c+l \in S$ for all $l \in \mathbb{N}$. We have $c \leqslant 2g$, and thus the "largest gap" of S is $l_g \doteq c-1 \leqslant 2g-1$, where $k \in \mathbb{N}$ is called a *gap of* S if $k \notin S$. The semigroup S is called *symmetric* when $r \in S$ if and only if $c-1-r \notin S$, for all $r \in \mathbb{Z}$. This is equivalent to say $c=2g$ (or $l_g = 2g-1$).

Write $S = \{\rho_1 = 0 < \rho_2 < \cdots\}$ as an enumeration of its elements in increasing order. With this notation, every $m \geqslant c$ is the $(m+1-g)$th element of S, that is $m = \rho_{m+1-g}$.

Definition 1. Let S be a numerical semigroup. For $m_1 \in S$, let $A[m_1] = \{p \in S \mid m_1 - p \in S\}$ and let $v[m_1] = \#A[m_1]$. The *Feng–Rao* distance of S is defined by the function

$$\delta_{\mathrm{FR}} : S \to \mathbb{N}, \quad \delta_{\mathrm{FR}}(m) \doteq \min\{v[m_1] \mid m_1 \geqslant m,\ m_1 \in S\}.$$

We now recall some well-known facts about the functions v and δ_{FR} for an arbitrary semigroup (see [11] or [13] for further details):

(i) $v[m] = m+1-2g+D(m)$ for $m \geqslant c$, where

$$D(m) \doteq \#\{(x,y) \in \mathbb{N}^2 \mid x, y \text{ are gaps of } S \text{ and } x+y=m\}.$$

(Note that the range $m \geqslant c$ is enough for coding theory purposes, since there one usually assumes that $m > 2g-2$.)

(ii) $\delta_{\mathrm{FR}}(m) \geqslant m+1-2g$ for all $m \in S$, and equality holds if moreover $m \geqslant 2c-1$.

In particular, it holds that $\delta_{\mathrm{FR}}(m) = v(m) = m+1-2g$ for all $m \in S$ such that $D(m) = 0$. If moreover S is symmetric, then we have

(iii) $\delta_{\mathrm{FR}}(m) = v(m) = m - l_g = m+1-2g = e$ for all $m = 2g-1+e$ with $e \in S \setminus \{0\}$ (see [3]).

Definition 2. Let S be a numerical semigroup. For $m_1, \ldots, m_r \in S$, let

$$A[m_1, \ldots, m_r] = A[m_1] \cup \cdots \cup A[m_r] = \{p \in S \mid m_i - p \in S \text{ for some } i = 1, \ldots, r\}$$

and $v[m_1, \ldots, m_r] = \#A[m_1, \ldots, m_r]$. For any integer $r \geqslant 1$, the rth *Feng–Rao distance* of S is defined by the function

$$\delta^r_{\mathrm{FR}} : S \to \mathbb{N},$$

$$\delta^r_{\mathrm{FR}}(m) \doteq \min\{v[m_1, \ldots, m_r] \mid m \leqslant m_1 < \cdots < m_r,\ m_i \in S\}.$$

Note that the classical Feng–Rao distance is $\delta_{\mathrm{FR}} \equiv \delta^1_{\mathrm{FR}}$. Very few results are known for the numbers δ^r_{FR}, even from a theoretical point of view, and they are completely scattered in the literature (see for example [2,8,14] or [19]). In the next section, we give the generalization of (ii) and (iii) for the general Feng–Rao distances.

3. Some general bounds and formulas

We first show that δ^r_{FR} behaves asypmtotically in the same way as the classical Feng–Rao distance up to a certain constant depending on S and r.

Theorem 3. *Let S be a semigroup with genus g and conductor c, and let $r \geqslant 2$. There exists an absolute constant $E_r = E(S,r)$ such that for $m \geqslant 2c-1$ we have*

$$\delta^r_{\mathrm{FR}}(m) = m + 1 - 2g + E_r.$$

Proof. Take $m_1 \geqslant m$ and $k_i > 0$ for $i = 1,\ldots,r-1$, and set $m_{i+1} = m_i + k_i$ for $i = 1,\ldots,r-1$. Denote $\mathbf{k} = (k_1,\ldots,k_{r-1})$. For fixed $\mathbf{k}$ and $h = 1,\ldots,r-1$, define the numbers

$$\gamma_{\mathbf{k}} \doteq \#\left\{ \lambda \in \mathbb{N} \setminus S \mid \lambda + \sum_{i=1}^{j} k_i \in S \text{ for some } j = 1,\ldots,r-1 \right\},$$

$$\mu^h_{\mathbf{k}} \doteq \#\left\{ l \in [1,k_h] \mid -l + \sum_{i=h}^{j} k_i \in S \text{ for some } j = h,\ldots,r-1 \right\}.$$

Note that $\gamma_{\mathbf{k}}$ does not depend on m_1, and if $m_1 \geqslant 2c-1$ then it equals to the number of integers in the interval $[0,m_1]$ which are not in $A[m_1]$ but belong to $A[m_i]$ for some $i \geqslant 2$. On the other hand, if $m_1 \geqslant c$ then the number $\mu^h_{\mathbf{k}}$ counts the elements of $A[m_1,\ldots,m_r]$ which are in the interval $[m_h+1, m_{h+1}]$. Thus, if $m_1 \geqslant m \geqslant 2c-1$ we check that

$$v[m_1,\ldots,m_r] = v[m_1] + \gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}} \tag{1}$$

and therefore, since neither $v[m_1]$ depends on $\mathbf{k}$ nor $\gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}}$ depends on m_1, in order to obtain the generalized Feng–Rao distance it suffices to compute independently the minimum of both quantities, and thus we get

$$\delta^r_{\mathrm{FR}}(m) = m + 1 - 2g + E(S,r),$$

where $E(S,r) \doteq \min\{\gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}} \mid k_i > 0 \ \forall i\}$. □

Definition 4. For $r \geqslant 2$, the constant $E_r = E(S,r)$, is called the rth *Feng–Rao number* of the semigroup S.

By definition we have that $r-1 \leqslant E(S,r) \leqslant r+g-1$, and hence $E(S,r) = r-1$ if $g = 0$. If $g > 0$ we have $E(S,r) \geqslant r$, and thus $E(S,r) = r$ if $g = 1$. On the other hand, for a fixed S the function $E(S,r)$ is non-decreasing in r, because of Theorem 3 and the fact that $\delta^r_{\mathrm{FR}}(m)$ is non-decreasing in r for a fixed m. A more precise bound is given in the following proposition.

Proposition 5. *Let S be a semigroup of genus $g > 0$, and let $r \geqslant 2$. Then*

$$r \leqslant E(S,r) \leqslant \rho_r.$$

If, furthermore, $r \geqslant c$ then $E(S,r) = \rho_r = r + g - 1$.

Proof. For the first statement it suffices to show the right-hand inequality. Let us note that $A[m] \subseteq A[m+p]$ for all pole orders $p \in S$. If $m \geqslant c$, then all the numbers $m+\rho_r-\rho_i$ are pole orders, $i=1,\ldots,r$, hence $A[m+\rho_r-\rho_i] \subseteq A[m+\rho_r]$ and consequently $A[m+\rho_r-\rho_1,\ldots,m+\rho_r-\rho_r] \subseteq A[m+\rho_r]$. Then, if $m \geqslant c$, by definition we have $\delta^r_{\mathrm{FR}}(m) \leqslant v[m+\rho_r]$. But $v[m+\rho_r] = m+\rho_r+1-2g$ when $m+\rho_r \geqslant 2c-1$. Thus,

$$\delta^r_{\mathrm{FR}}(m) = m+1-2g+E_r \leqslant m+\rho_r+1-2g$$

for $m \geqslant 2c-1$, hence $E_r \leqslant \rho_r$.

If furthermore $r \geqslant c$, then $\gamma_{\mathbf{k}} = g$ for all possible $\mathbf{k}$, and hence

$$E(S,r) = g + \min\left\{ \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}} \mid k_i > 0 \ \forall i \right\} = r+g-1$$

since this last minimum is achieved for $k_1 = \cdots = k_{r-1} = 1$. □

Remark 6. (1) The fact that $E(S,r) = \rho_r = r+g-1$ for $r \geqslant c$, shows that for large r the number $E(S,r)$ only depends on the number of gaps, and not on their distribution.

(2) The constant $E(S,r)$ can always be computed in a finite process. In fact, from the fact that $A[m] \subseteq A[m+p]$ for all pole orders $p \in S$, it suffices to consider $1 \leqslant k_i \leqslant \rho_2$, what requires to compute a minimum of a set with ρ_2^{r-1} elements, and one does not usually take r too large (in coding theory it suffices to consider $r \leqslant k$, where k is the dimension of the code; on the other hand $r \leqslant c$ because of Proposition 5). For the case $r=2$ the formula becomes much simpler, namely $E(S,2) \doteq \min\{\gamma_k + \mu_k \mid 1 \leqslant k \leqslant \rho_2\}$, where $\gamma_k \doteq \#\{\lambda \notin S \mid \lambda + k \in S\}$ and $\mu_k \doteq \#S \cap [0,k-1]$. Then, since $\mu_k = 1$ for $k \leqslant \rho_2$, we can write

$$E(S,2) = 1 + \min\{\gamma_k \mid 1 \leqslant k \leqslant \rho_2\}.$$

This formula is easy to compute in concrete examples with the aid of Apéry systems of generators, as we will show in the next section. In general, for $r > 2$ one could know such number from computing a suitable value of $\delta^r_{\mathrm{FR}}(m)$. For instance, $E(S,r) = \delta^r_{\mathrm{FR}}(2c-1) + 2g - 2c$. In this way, if moreover S is symmetric then $E_r = \delta^r_{\mathrm{FR}}(2g-1+e_0) - e_0$, according to Theorem 9 below.

(3) Although the bound $E(S,r) \leqslant \rho_r$ seems to be good, and it is sharp in many cases, it is not an equality in general, as we show in the following examples.

Example 7. (1) A semigroup S is said to be *elliptic* if $S = \langle 2,3 \rangle$ and *hyperelliptic* if $S = \langle 2,b \rangle$ for some odd integer b. If S is elliptic or hyperelliptic, it is easy to compute that $E(S,2) = 2 = \rho_2$ (that is, $\delta^2_{\mathrm{FR}}(m) = m+3-2g$ for $m \geqslant 2c-1$), hence we get equality in the bound $E(S,r) \leqslant \rho_r$ for $r=2$.

(2) Let $S = \{0,6,12,13,14,\ldots\}$ and $r=2$. A simple computation shows that $E(S,2) = 3 < \rho_2 = 6$.

We will show that the formula given in Theorem 3 is a lower bound for the generalized Feng–Rao distance from $m=c$, similarly to the case of the Feng–Rao distance.

Theorem 8. *Let S be a semigroup with genus g and conductor c, and let $r \geqslant 2$. Then, for $m \geqslant c$ we have*

$$\delta^r_{\mathrm{FR}}(m) \geqslant m + 1 - 2g + E(S,r).$$

Proof. If $c \leqslant m \leqslant 2c-1$, one has to replace $\gamma_{\mathbf{k}}$ in Eq. (1) by (1)′:

$$\gamma'_{\mathbf{k}} \equiv \gamma'_{\mathbf{k}}(m_1) \doteq \#\left\{ p \in S \mid m_1 - p \notin S \text{ but } m_1 - p + \sum_{i=1}^{j} k_i \in S \text{ for some } j = 1,\ldots,r-1 \right\}$$

(depending also on m_1). On the other hand, since $m_1 \geqslant c$, one has $v[m_1] = m_1 + 1 - 2g + D(m_1)$, where $D(m_1) \doteq \#\{(\alpha,\beta) \in \mathbb{N}^2 \mid \alpha,\beta \notin S \text{ with } \alpha + \beta = m_1\}$. Obviously $\gamma'_{\mathbf{k}} \leqslant \gamma_{\mathbf{k}}$, but if there is an element contributing to $\gamma_{\mathbf{k}}$ and not to $\gamma'_{\mathbf{k}}$ then it corresponds to a pair of gaps in $D(m_1)$, and thus $D(m_1) + \gamma'_{\mathbf{k}} \geqslant \gamma_{\mathbf{k}}$. As a consequence

$$v[m_1,\ldots,m_r] = m_1 + 1 - 2g + D(m_1) + \gamma'_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}} \geqslant m_1 + 1 - 2g + \gamma_{\mathbf{k}} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}}$$

and the theorem follows immediately from the definitions. □

We now study the case of symmetric semigroups. In this case, the conductor is $c = 2g$ and every m in the interval $[c, 2c-2] = [2g, 4g-2]$ can be written as $m = 2g - 1 + e$ with $e > 0$, so that $e \in S$ if and only if $D(m) = 0$, i.e., $\delta_{\mathrm{FR}}(m) = v[m] = m + 1 - 2g$ (see [3]). Hence, for those values the usual Feng–Rao distance equals to the Goppa distance. This can be generalized to the general case as follows.

Theorem 9. *Let S be a symmetric semigroup of genus g, and let $r \geqslant 2$. Let $m = 2g - 1 + e$ with $e \in S$ and $e > 0$. Then one has*

$$\delta^r_{\mathrm{FR}}(m) = m + 1 - 2g + E_r.$$

Proof. Let $\mathbf{k}_0$ any vector with $r-1$ non-zero components where the minimum E_r is achieved. For $m_1 = m$ one obviously has $\gamma_{\mathbf{k}} = \gamma'_{\mathbf{k}}$ for any vector $\mathbf{k}$, where $\gamma_{\mathbf{k}}$ and $\gamma'_{\mathbf{k}}$ are defined above. Then, take $m_1 < \cdots < m_r$ corresponding to m and $\mathbf{k}_0$, that is $m_1 = m$ and $\mathbf{k}_0 = (m_2 - m_1, \ldots, m_r - m_{r-1})$. We have

$$v[m_1,\ldots,m_r] = m + 1 - 2g + D(m) + \gamma_{\mathbf{k}_0} + \sum_{h=1}^{r-1} \mu^h_{\mathbf{k}_0} = m + 1 - 2g + E_r$$

since $D(m) = 0$ for such an m, and the theorem follows from the definitions and Theorem 8. □

Remark 10. We could try to mimic now the results of [3,13] for symmetric semigroups in order to find an interval (m_0, ∞) where the formula

$$\delta^r_{\mathrm{FR}}(m) = \min\{\rho \in S \mid \rho \geqslant m + 1 - 2g + E_r\}$$

is satisfied when $r > 1$. Following the techniques of [3], what we can say in principle is that

$$\delta^r_{\mathrm{FR}}(m) = \min(\{v[m_1, \ldots, v_r] \mid m_1 < m'\} \cup \{m' + 1 - 2g + E_r\})$$

m' being the minimum element in S of the form $m' = 2g - 1 + e'$ with $0 \neq e' \in S$. Unfortunately, the condition

$$v[m_1] \geqslant v[m'] \quad \text{for all } m \leqslant m_1 < m',$$

which is imposed in [3] to obtain a formula for m_0 when $r = 1$, is still necessary for $r > 1$ (since otherwise $v[m_1] < v[m']$ for some m_1 and by using Eq. $(1)'$ one would have $v[m_1, \ldots, m_r] < m' + 1 - 2g + E_r$ for a suitable choice of $\mathbf{k}$) but not sufficient. Then we cannot easily characterize the situation when such a formula is satisfied for an element m in a symmetric semigroup, and this still remains as an open problem for a general r.

4. Computing the second Feng–Rao number

Recall that for $r = 2$ we have $E(S, 2) = 1 + \min\{\gamma_k \mid 1 \leqslant k \leqslant \rho_2\}$. In order to compute this minimum, we shall use the theory of Apéry generators and relations (see [1,3]).

Definition 11. Let $S \subseteq \mathbb{N}$ be a numerical semigroup and let $e \in S$ non-zero. The *Apéry set of S related to e* is the set $\{a_0, a_1, \ldots, a_{e-1}\}$, where $a_i \doteq \min\{m \in S \mid m \equiv i \pmod e\}$, $0 \leqslant i \leqslant e - 1$.

Notice that $a_0 = 0$, and hence it does not give any essential information about S. The indices i can be identified to the corresponding elements in $\mathbb{Z}_{(e)} = \mathbb{Z}/e\mathbb{Z}$. Obviously, we have a disjoint union

$$S = \bigcup_{i=0}^{e-1} (a_i + e\mathbb{N})$$

and therefore the set $\{a_1, \ldots, a_{e-1}, e\}$ is a generator system for the semigroup S, which is called the *Apéry (generator) system of S related to e*.

Let $i, j \in \mathbb{Z}_{(e)}$ and consider $i + j \in \mathbb{Z}_e$; then $a_i + a_j = a_{i+j} + \alpha_{i,j}e$, with $\alpha_{i,j} \geqslant 0$, by definition of the Apéry set. The numbers $\alpha_{i,j}$ are called *Apéry relations*.

With these notations, every $m \in \mathbb{Z}$ can be written in an unique way as $m = a_i + le$, with $i \in \mathbb{Z}_e$ and $l \in \mathbb{Z}$. Then $m \in S$ if and only if $l \geqslant 0$. Thus, we can associate to any integer m two *Apéry coordinates* $(i, l) \in \mathbb{Z}_e \times \mathbb{Z}$, where the second one is non-negative just in the particular case when $m \in S$.

Moreover, the gaps of S can be described in terms of the Apéry system as follows: a positive integer β is a gap of S if and only if it can be written in the form $\beta = a_j - \lambda e$ for some $j \neq 0$ and $\lambda > 0$. More precisely, we define the numbers q_j by

$$a_j = j + q_j e$$

for $0 < j < e - 1$. Then the genus of S can be computed as $g = q_1 + \cdots + q_{e-1}$, and the set of gaps is $\{a_j - \lambda e \mid q_j > 0 \text{ and } 1 \leqslant \lambda \leqslant q_j\}$. Note that $q_j > 0$ is always true for $j \neq 0$ when $e = \min(S \setminus \{0\})$. In this way, we can prove the following

Proposition 12. *With the above notations, let $k = a_i + le$ a positive integer with Apéry coordinates (i, l) be given. Then we have*

$$\gamma_k = \sum_{q_j > 0} \min\{q_j, (l + \alpha_{i,j})^+\}$$

where $(l + \alpha_{i,j})^+ \doteq \max\{l + \alpha_{i,j}, 0\}$.

Proof. Let $\beta = a_j - \lambda e$ be a gap. Since $\beta + k = a_i + a_j + (l - \lambda)e = a_{i+j} + (\alpha_{i,j} + l - \lambda)e$, the condition $\beta + k \in S$ is equivalent to $\lambda \leqslant l + \alpha_{i,j}$. In order to count the number of gaps β such that the first Apéry coordinate equals to j and $\beta + k \in S$, we first note that if $l + \alpha_{i,j} < 0$ there exist no such a gap, since one must have $\lambda > 0$. On the other hand $\lambda \leqslant q_j$, and thus the searched number is just $\min\{q_j, (l + \alpha_{i,j})^+\}$, what yields the proposition by summing up in all the possible Apéry coordinates. □

In fact, since we are only interested in the numbers γ_k for $k = 1, \ldots, \rho_2$, from the above proposition we obtain the following

Corollary 13. *With the above notations, consider the Apéry system of S related to $e = \rho_2$. Then, for $k = 1, \ldots, \rho_2 - 1$ we have*

$$\gamma_k = \sum_{q_j > 0} \min\{q_j, (\alpha_{k,j} - q_k)^+\}$$

and $\gamma_{\rho_2} = \sum_{q_j > 0} \min\{q_j, 1\}$. *In this way, one can compute $E(S, 2)$ as*

$$E(S, 2) = 1 + \min\{\gamma_1, \ldots, \gamma_{\rho_2}\}.$$

Proof. If $e = \rho_2$, it suffices to note that for $k = 1, \ldots, \rho_2 - 1$, one has $i = k$ and $l = -q_k$, and for $k = \rho_2$ one has $i = 0$ and $l = 1$. Thus, the corollary follows from Proposition 12 and the fact that $\alpha_{0,j} = 0$ for all j. □

Example 14. Let us see how this formula works with a concrete example. Consider the semigroup $S = \langle 8, 10, 12, 13 \rangle$. It is telescopic (up to a permutation of the generators) and has genus $g = 14$ (see [13]). Take $e = \rho_2 = 8$ and the Apéry elements

$$a_1 = 25, \quad a_2 = 10, \quad a_3 = 35, \quad a_4 = 12, \quad a_5 = 13, \quad a_6 = 22, \quad a_7 = 23$$

(they can be derived from the telescopic structure, see [3]). Thus

$$q_1 = 3, \quad q_2 = 1, \quad q_3 = 4, \quad q_4 = 1, \quad q_5 = 1, \quad q_6 = 2, \quad q_7 = 2.$$

On the other hand, the non-zero Apéry relations are the following:

$$\alpha_{1,1}=5,\ \alpha_{1,3}=6,\ \alpha_{1,4}=3,\ \alpha_{1,5}=2,\ \alpha_{1,6}=3,\ \alpha_{1,7}=6,$$

$$\alpha_{2,2}=1,\ \alpha_{2,3}=4,\ \alpha_{2,6}=4,\ \alpha_{2,7}=1,\ \alpha_{3,3}=6,\ \alpha_{3,4}=3,$$

$$\alpha_{3,5}=6,\ \alpha_{3,6}=4,\ \alpha_{3,7}=6,\ \alpha_{4,4}=3,\ \alpha_{4,6}=3,\ \alpha_{5,5}=2,$$

$$\alpha_{5,7}=3,\ \alpha_{6,6}=4,\ \alpha_{6,7}=4,\ \alpha_{7,7}=3.$$

Now, we obtain the following values for γ_k, $k=1,\ldots,8$:

7 5 7 7 8 9 11 7

and hence the minimum is reached for $k=2$, that is $E(S,2)=6$.

Remark 15. In practical experiments with the computer algebra system Singular [7], the formula given by Corollary 13 is shown to be much more efficient (for large semigroups) than just computing the second Feng–Rao distance of a sufficiently large m in the semigroup and deducing the constant $E(S,2)$. As a comparison, if $S=\langle 9,13\rangle$, then Corollary 13 takes $E=9$ in less than 1 s, whereas computing the Feng–Rao distance for $m=104$ (the minimum element which can be taken to apply Theorem 9) by using the definition took us about 30 s.

In the sequel, we shall use a new characterization of $E(S,2)$ to obtain some more results on the second Feng–Rao number of S. In fact, for a positive integer k, let us consider the set

$$S_k=\{\rho\in S\mid \rho-k\notin S\}.$$

Obviously, $\#S_k=\gamma_k+1$, hence $E(S,2)=\min\{\#S_k\mid 1\leqslant k\leqslant \rho_2\}$. The following definition is due to Pellikaan [15].

Definition 16. A set $D=\{a+1,\ldots,a+t\}$ of t consecutive integers is called a desert of S if it verifies the two conditions

(a) $D\cap S=\emptyset$;
(b) $a\in S$ and $a+t+1\in S$.

Negative integers $-\mathbb{N}$ are also considered as the first desert of S. The set of deserts of S is denoted by $Des(S)$.

Let us observe that $\#S_1=\#Des(S)$, hence we have the bound $E(S,2)\leqslant \#Des(S)$. In some cases the above inequality is in fact an equality.

Example 17. (1) A semigroup S is said to be *hermitian-like* if $S=\langle a,a+1\rangle$ for some integer (not necessarily a prime power) a. A simple computation shows that for hermitian-like semigroups and $1\leqslant r\leqslant \rho_2$ we have $\#S_k=k(a-k+1)$, and hence $\min\{\#S_k\mid 1\leqslant k\leqslant \rho_2\}=\#Des(S)=a$.

(2) For some telescopic semigroups the result is true. For example, if $S = \langle 5, 6, 9\rangle$, a simple computation gives $\#S_1 = 4$, $\#S_2 = 6$, $\#S_3 = 6$, $\#S_4 = 6$, and $\#S_5 = 5$; thus

$$\min\{\#S_k \mid 1 \leqslant k \leqslant \rho_2\} = \#S_1 = \#Des(S) = 4$$

and hence $E(S,2) = \#Des(S)$. In some other cases, the equality does not hold. For example, if $S = \langle 5, 9\rangle$, we have $\#S_1 = 8$ and $\#S_5 = 5$ (see also Example 14).

For the semigroups shown in the above example, the computation of $E(S,2)$ has been simple. However, in the general case, the computation of $\min\{\#S_k \mid 1 \leqslant k \leqslant \rho_2\}$ seems to be very difficult. In what follows we shall offer some more results on this problem. In particular, we are able to compute this minimum for all semigroups generated by two elements.

Proposition 18. *Let S be a semigroup of genus g.*

1. *If $1 \leqslant k \leqslant \rho_2$ then $k \leqslant \#S_k \leqslant g + 1$.*
2. *If $k \in S$, then $\#S_k = k$.*

Proof. Every coset in $\mathbb{Z}/k\mathbb{Z}$ has a representative in S. Take the first one in each coset (that is, the 'Apery set' related to k, but note that we do not impose now $k \in S$). All these elements are in S_k, and hence $\#S_k \geqslant \#(\mathbb{Z}/k\mathbb{Z}) = k$. If $k \in S$ this first representative is also the only representative in S_k, and then $\#S_k = k$. If we now assume that $1 \leqslant k \leqslant \rho_2$, let us note that $\rho - k \notin S$ implies that either $\rho - k < 0$ or $\rho - k$ is a gap. Since there are exactly g gaps in S, we obtain the inequality $\#S_k \leqslant g + 1$. □

Let us study now the case of semigroups S generated by two elements, $S = \langle a, b\rangle$ with $a < b$ and $gcd(a,b) = 1$ (otherwise the semigroup does not have finite genus). The cases $a = 2$ and $b = a + 1$ are already studied in Examples 7 and 17, hence we can assume $2 < a < b - 1$.

Lemma 19. *Let $S = \langle a, b\rangle$ as above, and let $m, k \in \mathbb{N}$ such that $1 \leqslant k \leqslant a$ and $ma < l_g$. Then*

$$[ma, (m+1)a) \cap S_k \neq \emptyset.$$

Proof. If $m = 0$ the result is clear. For $m > 0$, let $d = gcd(a,k)$. We shall consider two cases according to whether the numbers a, k are relatively primes or not.

Case 1: $d = 1$. This implies that the integers $0, -k, -2k, \ldots, -(a-1)k$ are all different modulo a. Let us assume that $[ma, (m+1)a) \cap S_k = \emptyset$. Then, since $ma \in S$ one has that also $ma - k \in S$, and thus $ma - k + a \in S \cap [ma, (m+1)a)$. Again by hypothesis it follows that $ma - 2k + a \in S$, and now we have two possibilities: either $ma - 2k + a \in [ma, (m+1)a)$ or $ma - 2k + a < ma$. In the first case we continue with $ma - 3k + a$, and in the second case we continue with first $ma - 2k + 2a$ and afterwards with $ma - 3k + 2a$, obtaining anyway an element in $[ma, (m+1)a) \cap S$ which is congruent with $-3k$ modulo a. In this way, by iterating the procedure we obtain a different

elements in $[ma,(m+1)a)\cap S$, and hence $[ma,(m+1)a)\subseteq S$. Thus, one concludes that $\{n\in\mathbb{N}\mid n\geqslant ma\}\subseteq S$, contradicting the fact that $ma<l_g$.

Case 2: $d>1$. If $[ma,(m+1)a)\cap S_k=\emptyset$, a similar reasoning as in Case 1 shows that $[ma,(m+1)a)\cap S$ is the union of sets formed by all the representatives in $[ma,(m+1)a)_S$ of some classes modulo d. These classes include, at least, $0\,(\mathrm{mod}\,d)$ (because $ma\in S$) and $b\,(\mathrm{mod}\,d)$ (because $gcd(d,b)=1$, hence $a\,(\mathrm{mod}\,d)\neq b\,(\mathrm{mod}\,d)$). Since $[ma,(m+1)a)\cap S=\{b\,(\mathrm{mod}\,a),2b\,(\mathrm{mod}\,a),\ldots,tb\,(\mathrm{mod}\,a)\}$ for some t, and since $gcd(d,b)=1$, if all representatives of $b\,(\mathrm{mod}\,d)$ are in $[ma,(m+1)a)\cap S$, then $[ma,(m+1)a)\cap S$ contains some representatives (hence all possible representatives) of every class $(\mathrm{mod}\,d)$. Thus, as in the former case, we conclude that $[ma,(m+1)a)\subseteq S$, contradicting $ma<l_g$. □

Lemma 20. *Let a,b be as above. Then $(a-1)a<l_g$.*

Proof. Write $b=a+\alpha$, with $\alpha\geqslant 2$. Then $(a-1)(\alpha-1)\geqslant 1$ and we have

$$a(a-1)\leqslant a(a+\alpha)-a-(a+\alpha)=l_g. \qquad \square$$

Theorem 21. *Let $S=\langle a,b\rangle$ with $1<a<b$ and $gcd(a,b)=1$. Then*

$$E(S,2)=\min\{\#S_k\mid 1\leqslant k\leqslant a\}=\#S_a=a.$$

Hence, for $m\geqslant c$ one has $\delta^2_{\mathrm{FR}}(m)\geqslant m+1-2g+a$, and the equality holds for $m\geqslant 2c-1$.

Proof. It suffices to show that $\#S_k\geqslant\#S_a$ for all $k,1\leqslant k\leqslant a$. If $b=a+1$ this is already known. If $b>a+1$, and $1\leqslant k<a$, according to Lemma 20, we have $(a-1)a<l_g$, hence, according to Lemma 20, $\#S_k\geqslant a$ and the theorem is proved. □

Remark 22. (1) A natural question for semigroups generated by two elements is whether the formula

$$\delta^2_{\mathrm{FR}}(m)=\min\{\rho\in S\mid\rho\geqslant m+1-2g+E_2\} \tag{2}$$

is true for $m\geqslant 2g$ or not, generalizing the results of [13]. Unfortunately, it is not very difficult to find a counterexample for that. In fact, for $S=\langle 3,4\rangle$ with genus $g=3$, if one takes $m=7$ one has that $m+1-2g+E_2=5$, and thus the minimum element $\rho\in S$ with $\rho\geqslant 5$ is $\rho=6$. But the true Feng–Rao distance is actually $\delta^2_{\mathrm{FR}}(7)=v[7,8]=5$.

(2) However, it is easy to check that formula (2) is true in the range $m\geqslant 2g$ for the case of elliptic and hyperelliptic semigroups (see Example 7). In fact, if $S=\langle 2,c+1\rangle$, c being the conductor, it suffices to prove the formula for $m=c+\lambda$ with λ even and $\lambda\leqslant c-2$. Now by using Remarks 6 and 10, one must just check the minimum of the values

$$v[m,m+1]=v[m,m+2]=\frac{m}{2}+2 \quad\text{and}\quad \delta^2_{\mathrm{FR}}(m+1)=\lambda+4$$

(this last equality is obtained by Theorem 9, since $E_2=2$). We first consider the case $\lambda\leqslant c-4$. In this case one has $c\geqslant\lambda+4$ and hence

$$\frac{m}{2}+2\geqslant\lambda+4$$

but $\lambda+4$ is just the result of evaluating formula (2). For the case $\lambda=c-2$ one has $2+m/2=\lambda+3=c+1\in S$, and formula (2) is also satisfied.

References

[1] R. Apéry, Sur les branches superlinéaires des courbes algébriques, C.R. Acad. Sci. Paris 222 (1946) 1198–1200.
[2] A. Barbero, C. Munuera, The weight hierarchy of Hermitian codes, SIAM J. Discrete Math. 13 (1) (2000) 79–104.
[3] A. Campillo, J.I. Farrán, Computing Weierstrass semigroups and the Feng–Rao distance from singular plane models, Finite Fields Appl. 6 (2000) 71–92.
[4] A. Campillo, J.I. Farrán, C. Munuera, On the parameters of algebraic geometry codes related to Arf semigroups, IEEE Trans. Inform. Theory 46 (2000) 2634–2638.
[5] G.L. Feng, T.R.N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance, IEEE Trans. Inform. Theory 39 (1993) 37–45.
[6] G.D. Forney, Dimension/Length Profiles and Trellis complexity of linear block codes, IEEE Trans. Inform. Theory 40 (1994) 1741–1752.
[7] G.-M. Greuel, G. Pfister, H. Schoenemann, "SINGULAR", A computer algebra system for commutative algebra and algebraic Geometry; Available via http://www.singular.uni-kl.de.
[8] P. Heijnen, R. Pellikaan, Generalized Hamming weights of q-ary Reed-Muller codes, IEEE Trans. Inform. Theory 44 (1998) 181–197.
[9] T. Helleseth, T. Kløve, J. Mykkleveit, The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$, Discrete Math. 18 (1977) 179–211.
[10] T. Helleseth, P.V. Kumar, The weight hierarchy of Kasami codes, Discrete Math. 145 (1995) 133–143.
[11] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V. Pless, W.C. Huffman, R.A. Brualdi (Eds.), Handbook of Coding Theory, Vol. 1, Elsevier, Amsterdam, (1998) pp. 871–961.
[12] T. Kasami, T. Tanaka, T. Fujiwara, S. Lin, On complexity of trellis structure of linear block codes, IEEE Trans. Inform. Theory 39 (1993) 1057–1064.
[13] C. Kirfel, R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, IEEE Trans. Inform. Theory 41 (1995) 1720–1732.
[14] C. Munuera, On the generalized Hamming weights of geometric Goppa codes, IEEE Trans. Inform. Theory 40 (1994) 2092–2099.
[15] R. Pellikaan, Private communication.
[16] J. Simonis, Adding a parity-check bit, IEEE Trans. Inform. Theory 46 (2000) 1544–1545.
[17] M.A. Tsfasman, S.G. Vlăduţ, Algebraic-geometric codes, Math. Appl. 58 (1991).
[18] V. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inform. Theory 37 (1991) 1412–1428.
[19] K. Yang, P.V. Kumar, H. Stichtenoth, On the weight hierarchy of geometric Goppa codes, IEEE Trans. Inform. Theory 40 (1994) 913–920.